Information Theory, Fall 2014 Iftach Haitner

Problem set 4

December 24, 2014 Due: January 6

- Please submit the handout in class, or email the grader.
- Write clearly and shortly using sub-claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- It is allowed to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase")

1. Let $\mathcal{G} = \{(A, b) \in \{0,1\}^{m \times n} \times \{0,1\}^m\}$ be the function family from $\{0,1\}^n$ to $\{0,1\}^m$, defined by $(A, b)(x) = A \times x + b$, where all operations are over $\mathbb{F}_2$ (i.e., modulo 2).

   Prove that $\mathcal{G}$ is a pairwise independent function family.

2. Prove Claim 13 of Lecture 9